# Ex. 13
# James Mickens Opening Opinion Summaries

[redacted]

## II. Summary of Expert Opinion

13. My expert opinion is that iPhone security is in fact significantly independent of the review process and the distribution channel (however they may be implemented). It is therefore my expert opinion that Apple considerably overstates the security benefits of its own centralized App Store model.

14. As the rest of this document explains in detail, the iPhone's security guarantees could predominantly be enforced by the iPhone's operating system (iOS), not by the Apple App Store. In practice, iPhones do indeed mostly rely on iOS to achieve Apple's stated security goals.

15. In theory, Apple's review guidelines enumerate some security properties that cannot be enforced by an operating system alone; however, a variety of empirical evidence suggests that, in practice, the App Store does a weak (at best) job of enforcing these additional security properties. My overall conclusion is that, if Apple allowed iPhone users to opt into app distribution via third-party channels, those users would not suffer from a meaningfully less-secure experience.

16. I now summarize my opinion in more detail. I believe that the Apple-mandated review process and distribution channel try to enforce five security properties for iPhone apps: sandbox compliance, exploit resistance, malware exclusion, user consent for private data access, and legal compliance. As I demonstrate in Section IX, the first three properties (sandbox compliance, exploit resistance, and malware exclusion) are entirely enforceable by an operating system alone, without assistance from an Apple-style review process and centralized distribution channel. The fourth and fifth properties (user consent for private data access, and legal compliance) can only be partially enforced by an OS alone. However, and importantly, the security properties which an OS cannot enforce are also difficult for Apple's App Store to enforce. In practice, this means that the Apple-controlled App Store provides minimal additional benefit relative to the security guarantees that could be provided by iOS.

[redacted]

17. Note that iOS is already capable of loading apps that were not reviewed by Apple; thus, Apple tacitly already acknowledges that OS-based security mechanisms are the fundamental way that Apple keeps users safe. In particular, the Apple-sanctioned Developer Enterprise program[5] allows a third-party business to distribute the company's proprietary apps to company employees. These apps are not reviewed by Apple. Although the third-party company acts as a direct distribution channel, iOS is still able to provide its traditional security guarantees. The reason is that enforcement of those security guarantees is largely independent of how an app arrives on a device (and whether the app was reviewed before distribution).

18. Apple allows MacOS computers to download third-party apps directly from user-selected distribution channels. Those apps may not have been reviewed by Apple. However, MacOS and iOS protect many of the same kinds of user data (e.g., emails, financial information, and web browsing histories). This data requires safeguarding on both iPhones and MacOS devices. The fact that Apple allows MacOS computers to install third-party applications from user-selected distribution channels is another tacit admission that Apple primarily relies on the OS, not the app distribution mechanism, to enforce security guarantees.

19. iPhones do have sensor hardware (e.g., GPS units and accelerometers) that MacOS devices typically lack. These sensors generate data about an iPhone user's current physical environment; such data is obviously sensitive. However, Apple allows data syncing between a user's iPhone and MacOS devices. The syncing mechanisms, which are implemented by Apple, provide MacOS with a sanctioned access path to a user's iOS-generated data. Thus, Apple is tacitly comfortable with iOS-generated data being accessed by third-party MacOS apps that may not have been reviewed by Apple.

20. iPhones use curated, centralized app distribution. In contrast, Android devices allow third-party distribution channels (subject to certain restrictions beyond the scope of this report). Apple often touts the purportedly stronger security of iPhones over Android devices. However, a variety of evidence suggests that iPhones are not significantly more secure than Android devices. For example, a recent security evaluation of hundreds of iPhone apps found that those apps suffered from many of the security problems observed in Android apps. As another example, the open market for smartphone security vulnerabilities currently assigns a higher monetary value to Android security exploits. These market dynamics imply that Android is actually *more secure* than iOS.

21. Most vendors of popular consumer devices work hard to make their devices secure; Apple is no exception. As I explain throughout the report, Apple's most important security mechanisms have direct (or very close) analogues in competing platforms like Windows, Android, and Linux. Apple's reputation for caring about security is not undeserved, but hyperbolically superlative assessments of Apple's security in the popular media are partially driven by historical beliefs that are no longer true. When iPhones were first introduced in 2007, Microsoft was still struggling with a variety of Windows

[5] See Paragraph 121 for details about the Developer Enterprise program.

[redacted]

security problems, and Google had not yet made Android security a topmost priority. Fourteen years ago, Apple's focus on security was somewhat unique. However, the modern status quo is different. The vendors who make popular smartphones, desktops, and laptops now understand that computers are ubiquitous and process a variety of sensitive user data. There is now wide agreement that making devices secure is a critical priority. A key conclusion of this report is that, to the extent that Apple can enforce the aspirational security properties enumerated by Apple's review guidelines, the enforcement mechanisms are well-known and are used by non-Apple platforms too. Thus, Apple's general claims of providing a radically safer user-experience are unwarranted. I understand that Professor Wenke Lee has prepared an expert report which addresses in more detail the extent to which a third party could replicate the claimed security-related aspects of Apple's app review.

22. Apple's app review process examines some app characteristics which are not security-related, but which Apple still perceives as desirable to customers or to Apple's own business interests. In general, an OS cannot determine whether apps possess these characteristics. For example, Apple's review process filters out apps that contain objectionable content like religiously-offensive images; an OS is typically incapable of identifying such material automatically. As another example, Apple's review process rejects apps that do not provide "lasting entertainment value."[6] The definition of "lasting entertainment value" is inherently subjective and therefore best evaluated by a human reviewer.

23. However, based on Apple's public-facing descriptions of its review process, I believe that this kind of subjective app evaluation could be implemented by a third-party app store. For example, any reasonable person can determine whether an app provides "lasting entertainment value"; being an employee of Apple is not a bona fide occupational qualification for issuing such a judgment. Thus, a third-party app store could hire its own evaluators to determine whether an app provides "lasting entertainment value." As another example, Apple's review process determines whether an app has a visual design which satisfies Apple's aesthetic goals of "clarity," "deference," and "depth."[7] A third-party app store is capable of employing workers who can determine whether an app satisfies a particular aesthetic philosophy.

24. As a concrete example of such a third-party app store, consider GOG, a curated online game store usable by personal computers running MacOS, Windows, or Linux.[8] GOG, like Apple, takes an opinionated stance on various aspects of the distribution process—but GOG has different opinions than Apple. For example, GOG's explicitly-stated goal is to provide a "curated selection of games" which satisfy (1) GOG's aesthetic sense of "entertainment value," and (2) GOG's preference for games that do not require users to

[6] See Section 4.2 of Apple's review guidelines. "App Store Review Guidelines." Apple Developer. Apple. Accessed on February 14, 2021. https://developer.apple.com/app-store/review/guidelines/.

[7] See Apple's human interface guidelines. "Human Interface Guidelines." Apple Developer. Apple. Accessed on February 14, 2021. https://developer.apple.com/design/human-interface-guidelines/ios/overview/themes/. Adherence to the human interface guidelines are described as a mandatory part of compliance with the overall review guidelines; see "App Store Review Guidelines." Apple Developer. Apple. Accessed on February 14, 2021. https://developer.apple.com/app-store/review/guidelines/.

[8] Gog. Accessed on February 14, 2021. https://www.gog.com/.

[redacted]

install DRM technology.[9] Like Apple, GOG tests games before distributing them. However, unlike Apple, a portion of GOG's offerings are very old games that were not designed for modern computers. Because supporting old games is an explicit goal of GOG's app store, GOG will try to fix app bugs or performance issues that GOG discovers during its review process.[10] This approach contrasts with that of Apple, which simply rejects apps that are found to be buggy during Apple's app review. The point is not that GOG's approach is "the right one" and Apple's approach is "the wrong one"; instead, the point is that users and developers benefit from the opportunities provided by app store choice.

25. The rest of my report is organized as follows: Section III provides a high-level overview of the way that computers operate, explaining the relationship between hardware and software. Section IV gives a high-level overview of a particular kind of software called an operating system. The operating system acts as a computer's manager, orchestrating the interactions between different apps and different hardware devices. Section IV's broad discussion of operating systems is followed by a deeper dive in Section V, where I furnish details about how an operating system keeps apps secure. In Section VI, I discuss a particular type of app called a "signed app". A signed app uses cryptography to prove that a specific actor (e.g., a developer or a company) vouches for the content in the app; Apple requires an iOS app to be signed. Given all of this background information about computer design, operating system design, and signed applications, I then explain how iOS in particular enforces various security properties (Section VII). Section VIII then describes how Apple's App Store operates. I conclude in Section IX that Apple's review process confers few practical benefits to app security.

[9] DRM (digital rights management) technology refers to hardware and/or software that restricts how users interact with digital content. For example, after a user purchases a game, DRM technology could limit the set of user-owned devices on which the user can play the game. A "DRM-free game" is one that, once purchased by a user, can be played on any device.

[10] As GOG states at https://www.gog.com/about_gog, "Even if the game is older than you are, we test it thoroughly, fix all the bugs, and apply patches so it runs flawlessly on your next-gen PC and on modern OSs."